STRATEGY RESEARCH PROJECT

INFORMATION WARFARE: THE ORGANIZATIONAL DIMENSION

BY

COLONEL BRIAN FREDERICKS
United States Army

USAWC CLASS OF 1996

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INFORMATION WARFARE: THE ORGANIZATIONAL DIMENSION

by

Colonel Brian Fredericks
United States Army

Mr Robert F. Minehart, Jr.
Project Adviser

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Brian E. Fredericks (COL), USA

TITLE: Information Warfare: The Organizational Dimension
FORMAT: Strategy Research Project

DATE: 7 February 1996 Pages: 22 CLASSIFICATION: Unclassified

Since the December 1992 publication of the Department of Defense (DOD) classified directive on Information Warfare (IW) considerable effort has been expended examining this issue. Despite this attention, a clear vision for the implementation of IW within DOD and the U.S. Government as a whole has yet to emerge. Three pillars are essential to achieving a viable IW strategy and supporting architecture: policy/doctrine, organization/training, and requirements/technology. Much has been written, discussed, and even debated on the need for overarching national policy in this area, as well as the multitude of capabilities and vulnerabilities stemming from our increased reliance on advanced technology. A similar focus on the organizational component of IW has not occurred. The study specifically addresses the role of organizations as a key component of IW. Both the progress achieved to date within DOD and the significant challenges remaining to be overcome at the interagency level are examined. Specific recommendations are provided on how better to organize the IW effort.

Introduction

Today with all of the various interpretations and multiple definitions, Information Warfare (IW) remains an enigma. Since the Department of Defense formally published the original classified directive on IW in December 1992, the Services, Office of the Secretary of Defense, and a wide range of joint activities have expended considerable effort examining this issue. While there is a general recognition that IW has the potential to serve as an important force multiplier, the concept remains in its infancy. Ultimately the success of IW as a decisive component of U.S. national security in the 21st century depends upon achieving a viable IW architecture. This architecture must comprise three key areas: policy/doctrine, organization/training, and requirements/technology. Much has been written, discussed, and even debated on the need for overarching national policy in this area, as well the multitude of capabilities and vulnerabilities stemming from our increased reliance on advanced technology. However, a similar focus on the organizational component of IW has not occurred.

This paper specifically addresses the role of organizations as an essential element in developing and implementing a viable IW strategy. To provide a common reference point, the paper begins by defining IW. Next it analyzes the progress achieved to date in institutionalizing IW by assigning responsibility to specific organizations. Both the progress achieved within DOD and the significant challenges remaining to be overcome at the interagency level are examined. The paper concludes with a set of recommendations on how to better organize the IW effort and enable it to emerge as a decisive element of U.S. national security strategy in the 21st century.

IW Defined

Information Warfare (IW) was formally launched in December 1992 with the dissemination of DOD Directive 3600.1.[1] From the outset, widespread discussion and understanding of IW were hampered by its Top Secret classification.[2] In September 1995 the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) published the

formal DOD unclassified definition of IW:

> Actions taken to achieve information superiority by affecting adversary information,information-based processes, and information systems, while defending one's own information, information-based processes, and information systems.

This description clearly underscores both the defensive, as well as offensive aspects of IW. In the summer of 1994, the Defense Science Board[3] (DSB), drawing heavily from expertise within DOD, published the most comprehensive and authoritative discussion of IW to date. The report highlighted the distinction between information in warfare and information warfare. Information in warfare pertains to "getting [information] it where it is needed in a timely and reliable manner.[4]" It encompasses the collection, processing, and dissemination of information and is synonymous with the "C4I for the Warrior" vision released by the Joint Staff in 1992. C4I for the Warrior addresses the concept of a global Command, Control, Communications, Computer, and Intelligence system directly linking military units around the globe in an interoperable, fully integrated fashion spanning the range of military operations from peace to war.[5]

Information in warfare capitalizes on the national information infrastructure (NII). Characterized as an "information highway,[6] the NII is the growing worldwide information infrastructure which transcends industry, media, and the military and includes government and non-government entities. Most activities now rely on the information infrastructure including the banking, transportation, manufacturing, and electrical power industries. The Defense Information Infrastructure (DII) is an integral part of the NII with over 95 percent of DOD's worldwide telecommunications needs satisfied by commercial telecommunications carriers.[7] Military activities relying on the DII include transportation, logistics, financial, manpower, and personnel and training.

While C4I for the Warrior focuses on harnessing ever-increasing computer storage and exchange capabilities, IW targets these information systems. The distinction between C4I for the Warrior and IW is extremely important. IW employs offensive techniques such as deception, electronic jammers, munitions and advanced technologies to deceive, deny, exploit, damage, or destroy adversary

information systems, while at the same time protecting friendly information systems from disruption, exploitation and damage by an adversary .[8] The target of IW may range from influencing national level decisionmakers to corrupting the automated control of transportation systems.[9] defensive IW protects friendly information systems from disruption, exploitation and damage by an adversary .[10] For example, the Army's ongoing digitization of the battlefield is an application of information in warfare at the operational and tactical levels. Defensive IW, on the other hand, focuses on identifying and protecting vulnerabilities which arise from this increased reliance on technology.

The emergence of Command and Control Warfare (C2W) has been fundamental in understanding IW.[11] In an article in Signal magazine LTGen James Clapper, then Director Defense Intelligence Agency (DIA), wrote "the closest description of information warfare might be found in the definition of command and control warfare."[12] IW and C2W, however, are not interchangeable terms. C2W is a subset of IW. The Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30, states "C2W is the military strategy which implements IW on the battlefield."[13] C2W is designed as an essential part of an overall theater campaign plan. It is implemented during "joint military operations when U.S. military forces unilaterally or as part of an allied/coalition force are opposed or threatened by an organized military or paramilitary force."[14] C2W focuses on an adversary's military command and control when military force is applied. On the other hand, the use of the word "warfare" in the term IW does not limit IW to a military conflict, declared or otherwise.[15] IW targets the entire information infrastructure of an adversary - political, economic, and military throughout the continuum of operations from peace to war.

Organizational Imperative

IW, as this definitional discussion highlights, is a complex issue. Organizations are essential in actually implementing this new concept and achieving a viable IW architecture. IW will only become institutionalized if activities actually take responsibility for planning and executing IW. Today IW offices have been stood up throughout DOD focusing on offensive and defensive IW capabilities, but for

the most part the budgets and staffs of these elements are very limited. They represent an important start in what will likely be a long and slow process.

IW Executive Board: The Deputy Secretary of Defense chairs an IW Executive Board established in May 1995 which comprises senior officials within the department including the Vice Chairman Joint Chief of Staff (VCJCS)[16]. Supporting the IW Executive Board is an IW Council chaired by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)). The Executive Board is chartered to address IW roles and responsibilities and serve as the DOD focal point for IW discussion at the national level. The Board is a welcome addition as it demonstrates an awareness by senior DOD officials of the need to coordinate IW, not only within the department, but in the interagency arena. However, senior officials are too busy to spend a great deal of time on any one issue, particularly one that has not reached crisis proportions. This is the point Robert McNamara makes in his book In Retrospect when discussing the evolution of U.S. policy in Vietnam during the Kennedy and Johnson administrations and the same is true today.[17] You need to have the pull from the top, but it is important that lower levels are fully energized.

ASD C3I : The ASD(C3I), as the senior IW advisor to the Secretary of Defense, has organized a small IW Directorate comprising less than ten personnel to help him execute his responsibilities. It was the forerunner to this office which drafted the original IW directive in 1992. The IW Directorate conducts centralized planning, coordination, and oversight for IW and conducts program reviews of selected Service and defense agency IW efforts. In May 1995 the IW Directorate sponsored an IW wargame for senior government officials designed to raise the profile of the threat to the U.S. information infrastructure.[18]

The IW Directorate has also focused on initiating a DOD "Red Team" effort. This was one of the IW recommendations from the 1994 Defense Science Board report to "jump start Defensive IW."[19] Under this concept personnel knowledgeable in adversaries' offensive IW form a team to "attack" the DOD information infrastructure. Given the magnitude of the vulnerabilities, the objective would be to

have this capability distributed throughout DOD and carried out at various levels and locations. This concept dovetails with the Computer Emergency Response Team (CERT) which reacts to real world intrusions into computer systems. The Defense Information Systems Agency (DISA) has stood up small offices which accomplish both these tasks, but a more comprehensive program is necessary. In the twelve months prior to July 1994 DISA detected roughly 3,600 attacks on military networks, but officials estimate they detected only two percent of all the attacks, raising the estimated number to 182,000.[20]

The "Red Team" program is designed to increase awareness throughout DOD of the vulnerabilities of automated systems and improve the overall security posture. A comprehensive "Red Team" effort can significantly reduce vulnerabilities in the near term as many existing problems are attributed to inadequate training of operators and system administrators. As the head of a CERT team stated, "the problem...is a lack of understanding and awareness and a lack of training and technical competence on the part of the user community."[21] The "Red Team"is a laudable objective, but ASD(C3I) presently only coordinates and does not direct action. The Joint Staff has designated the Joint Command and Control Warfare Center (JC2WC) at San Antonio, Texas as executive agent to support the OSD IW Red Team effort. However, implementation of the "Red Team" concept is evolving slowly given budget constraints and manpower reductions in the Services and defense agencies.

USD(P): In 1995 the Under Secretary of Defense (Policy) (USD(P)) created an Infrastructure Policy Directorate. This office focuses on emergency preparedness and shaping the role of DOD in the protection of infrastructures, including coordination between DOD and non-DOD government, and civilian/corporate owned infrastructures.[22] These are important responsibilities which clearly fall under the heading of defensive IW. As this office matures, it will be incumbent upon the IW Council and Executive Board to insure IW activities within ASD(C3I) and USD(P) are delineated and deconflicted, if necessary.

Joint Staff: In the Joint arena, IW organizations have also emerged. On the Joint Staff,

proponency for IW is now shared between the Directorate for Operations, J3, and the J6, Directorate for Command, Control, Communications, Computers, and Intelligence (C4I) under a Memorandum of Understanding signed in October 1994. While conceptually this may have merits with each directorate bringing a unique dimension of IW, in reality as Lt Gen Clapper, former Director, DIA, has recommended, the Operations Officer should be the overall staff coordinator as he is for all other operations issues.[23]

The current arrangement on the Joint Staff presents some unique challenges as no one is actually in charge. The J3 and J6 principals are too busy to dedicate the constant attention this area requires and day-to-day responsibility for IW on the Joint Staff is delegated. A need exists for direct flag officer sponsorship to orchestrate joint IW policy and doctrine development, conduct operational planning, and establish requirements. A dedicated flag officer sponsor would greatly facilitate coordination with Services, OSD, the Intelligence Community and as IW matures, the interagency and civilian sectors. It would also send a strong message that IW is an important joint warfighting issue requiring immediate high-level attention.

Within the Joint Staff J3, responsibility for offensive IW now resides within the Information Warfare /Special Technical Operations Division (IW/STOD). This division is responsible for coordinating compartmented planning between the Services, Combatant Commands, and DOD agencies. Bob Woodward writes in The Commanders, the Special Technical Operations Center (STOC) is "a command and communications center for operations involving the sensitive "black" programs known only to those cleared to the special-access compartments."[24] The IW/STOD also has responsibility for coordinating all facets of C2W for the Joint Staff including policy, doctrine, and operational issues. It is this office which authored MOP 30, led the preparation of Joint Pub 3-13 and will draft IW doctrine. This arrangement underscores the important linkage between C2W and IW. As the military proceeds to operationalize IW, the IW/STOD represents the linchpin for ensuring the integration of all dimensions of joint IW.

It has been suggested that, just as we continue to use a Single Integrated Operational Plan (SIOP) for strategic nuclear warfare, DOD might consider the use of an "IW SIOP" which addresses offensive and defensive deconfliction and intelligence equity issues.[25] If this were implemented, the task would be assigned to the IW/STOD to coordinate the task. Today the IW/STOD focuses principally on support to the Combatant Commands, but as IW matures with both its non- lethal and deterrence potentials, greater interagency participation and coordination will undoubtedly occur.

JC2WC: The activation of the Joint Command and Control Warfare Center (JC2WC) at San Antonio, Texas in October 1994 provided a valuable resource for the Commanders of the Combatant Commands (CINCs).[26] As a field-operating agency of the Joint Chiefs of Staff and headed by a flag officer,[27] the JC2WC is fully engaged in the warfighting application of IW. With 163 assigned personnel, the JC2WC dispatches tailored teams to augment CINC and Joint Task Force staffs and provide C2W expertise in all joint exercises and contingency operations. Personnel from the JC2WC have participated in U.S. efforts in Bosnia and contingency operations in both Kuwait and Haiti. Given the high turnover of personnel on CINC staffs, the JC2WC is very much in demand for its C2W expertise.[28]

The JC2WC is in the unique position of being able to cross fertilize and share C2W lessons learned between the Combatant Commands. Accordingly, the organization has played a major role in developing joint C2W doctrine and will contribute significantly to the preparation of a follow-on C2W Joint Tactics, Techniques, and Procedures (JTTP) publication. At the present time, the JC2WC is fully engaged accomplishing its assigned tasks with respect to C2W. It is only now beginning to analyze its newly assigned responsibilities as executive agent in support of the OSD IW Red Team effort. As IW evolves and DOD's role in the larger IW arena is clarified, a natural progression will be for this organization to serve as the nucleus for a Joint IW center.

Joint COMSEC Monitoring Activity. The JCMA is another field operating agency of the Joint Chiefs of Staff having IW applications. It was created in 1993 by a Memorandum of Agreement

between the Service Operations Deputies and Directors of the Joint Staff and NSA. The JCMA is charged with conducting "COMSEC monitoring (collection, analysis, and reporting) of DOD telecommunications and automated information systems (AIS) and monitoring of related noncommunications signals."[29] Its purpose is to identify vulnerabilities exploitable by potential adversaries and recommend countermeasures and corrective actions. The JCMA focuses on unencrypted DOD systems and "does not perform traditional telephone monitoring," as this function remains a Service responsibility.[30] The Joint Staff Director for Operations has been assigned primary responsibility for JCMA affairs. This facilitates coordination between the JC2WC and the JCMA. The JCMA supports both real-world operations, as well as joint exercises and DOD systems monitoring. The JCMA, more so than the JC2WC, already has the expertise to perform the Red Team mission. Rather than further diluting the already stretched resources and expertise of the JC2WC, it would make better sense to designate the JCMA as executive agent to support the OSD Red Team IW initiative.

Joint Spectrum Center. The DOD Joint Spectrum Center (JSC) was activated in September 1994 under the direction of the Joint Staff J6. The JSC assumed all the mission and responsibilities previously performed by the Electromagnetic Compatibility Center, as well as additional functions. The JSC deploys teams in support of the CINCs and serves as the DOD focal point for supporting spectrum supremacy aspects of IW. Notably the JSC assists warfighters in developing and managing the Joint Restricted Frequency List (JRFL) and assisting in the resolution of operational interference and jamming incidents. While informal coordination occurs on IW related issues between the Joint Spectrum Center, the Joint COMSEC Monitoring Activity, and the Joint C2W Center, each organization interfaces separately with the CINC staffs. No formal mechanism is yet in place to ensure the warfighters obtain a coordinated IW support package.

Combatant Commands: The focus of warfighters at the Combatant Commands remains planning and executing C2W. All of the geographic CINCs now have C2W staff officers assigned in their Operations Directorates, but organizing the diverse elements which comprise C2W is a challenge

for CINC staffs. U.S. Central Command (CENTCOM) has actually physically consolidated the staff officers responsible for orchestrating electronic warfare, operational security, military deception and psychological operations into a single branch. This organization can serve as the nucleus as new IW capabilities emerge and are apportioned to the CINCs. Defensive IW poses a more significant challenge. While the CINCs can take incremental measures to unilaterally reduce vulnerabilities of their information systems, given their ultimate dependence on the national information infrastructure, defensive IW must be undertaken as part of a larger DOD sponsored initiative.

Services: Each of the Services have created or are participating in Information Warfare Centers or Activities. The Air Force leads the Services and in September 1995, the Chief of Staff and Secretary of the Air Force published the 17 page, Cornerstones of Information Warfare which describes how "Air Force doctrine should evolve to accommodate information warfare."[31] The Air Force was also the first to establish their Information Warfare Center (AFIWC) at San Antonio, Texas in October 1993. This was accomplished by consolidating the Air Force cryptologic support center and the electronic warfare center. The AFIWC serves as the Air Force command and control warfare executive agent with approximately 1000 military and civilian personnel assigned. The Center is subordinate to the Air Intelligence Agency closely aligning it with the Intelligence Community. The Center applies the teaming concept integrating the intelligence component with operators, engineers, communications and computer specialists, both offensive and defensive.[32] The AFIWC also has an ongoing "Red Team" and CERT effort designed to improve network security in the Air Force. The Center is collocated with the JC2WC and both organizations work closely together. Personnel from the AFIWC regularly team with the JC2WC on major deployments.

On 1 October 1995, the Air Force created its first Information Warfare Squadron at Shaw Air Force Base, South Carolina. The squadron's primary purpose will be to protect Air Force computers and communications, as well as assisting in "infiltrating an enemy's computer and communications systems."[33] The squadron will support the 9th Air Force commander who is assigned the Central

Command area of operations. Eventually, the Air Force will set up more squadrons to assist air commanders responsible for other geographic areas. While the IW Squadron at Shaw AFB presently only has two officers assigned, there will be as many as 40 by August 1996, when the squadron is slated to be operational. Eventually, the squadron might grow to 85 people.[34] The Air Force recognizes it is pushing the envelope, but as General Joseph Ralston, chief of Air Combat Command, stated:

> You can sit around for another 10 years and debate about what some of the problems might be [with setting up an information warfare squadron]...but you will never know until you actually get into them and try to make it work operationally.[35]

The Navy established the Navy Information Warfare Activity (NIWA) in August 1994 to serve as their focal point for IW activities.[36] Directly subordinate to the Naval Security Group, the NIWA is located at Fort Meade, Maryland and is closely linked to the National Security Agency.

Given the rapid pace of advancing technology the Navy has given the NIWA special authority to generate requirements and procure systems. Traditionally there has been a sharp separation in the Navy between organizations responsible for setting requirements and those charged with overseeing their acquisition. However, with new generations of computers and information systems unveiled on average about every 18 months, the Navy has adopted a more streamlined approach. As John Davis, technology adviser to the Navy's Space and Electronic Warfare Directorate, indicated, "If we fall more than one cycle behind. we could find industry putting information warfare systems into potentially hostile nations at the same time that US force receive the same equipment."[37]

The Navy also has established the Fleet Information Warfare Center (FIWC) at Little Creek, Virginia from existing Fleet Deception/C2W Group assets.[38] The FIWC serves as the link between the NIWA and the Atlantic and Pacific Fleets. With personnel deployed on carrier battle groups throughout the world, the FIWC fulfills a similar mission for the Navy that the JC2WC does for the joint warfighter. The IW organizational structure created by the Navy enables the FIWC to focus on near term operational requirements, while the NIWA assumes a more long-term perspective keeping abreast of IW advances and developing and acquiring systems.

Rather than create a separate IW organization, the Marines intend to assign liaison officers to the respective Service IW centers to benefit from their efforts. The Navy and Marines have also teamed up to develop policy guidance for Navy and Marine IW/C2W operations. In February 1995, the Marine Corps Commandant and Chief of Naval Operations approved a plan which states, "Navy and Marine Corps must have a fully integrated IW/C2W capability...team must organize, train, and equip its forward deployed forces to conduct IW/C2W."[39]

The Army is the latest Service to establish an IW activity. Officially activated in May 1995, the Land Information Warfare Center (LIWA) is subordinate to the Army Intelligence and Security Command (INSCOM) but is under the operational control of the Headquarters Department of the Army, Deputy Chief of Staff for Operations (DCSOPS). As with the Air Force and Navy, the Army has closely aligned its IW effort with the Intelligence Community. The LIWA is a totally new organization in contrast to the Air Force and Navy efforts which reorganized existing activities. It is also the smallest of the three Service IW activities with a projected end strength of 50-75 personnel. The primary focus of the LIWA is to provide operational support at the Army Corps and higher levels. The Army is also coordinating closely with the Marines to assign personnel to the LIWA. Given its small size, the LIWA draws upon existing capabilities in the Army including psychological operations, electronic warfare, and operational security. The Army is in the process of institutionalizing a "Red Team" effort from existing INSCOM assets, and there is close coordination and collaboration with NSA on mutual IW efforts.

The Services' efforts during a period of serious budget constraints underscore a recognition of the importance of IW. Except for the general responsibilities delineated in the original DOD IW directive, Services have received no additional policy guidance on how to implement IW. In reviewing Service responses to IW, they have established organizations which best suit their near term needs. Manpower and funding for Service IW initiatives have been reallocated internally with the Air Force taking the most aggressive approach.

Over time Service organizations can be expected to evolve as IW matures. Today much of their

focus is on implementing C2W, the military application of IW. Services have also implemented "Red Teams" to train personnel and improve security awareness of the vulnerabilities associated with information systems. Additionally, while the linkages of Service IW organizations with the Intelligence Community is valuable, it is important IW does not become an intelligence activity. IW needs to be controlled and fully managed by the warfighters as an integral part of an overall strategy. In that regard, the recent activation of the IW Squadron by the Air Force, separate and distinct from the AFIWC, is a positive step.

Intelligence Community: Within the Intelligence Community there exists an acute appreciation of the enormous impact IW has on their efforts. Each organization, DIA, CIA and NSA has established an office to orchestrate IW related activities and satisfy the needs of their consumers. NSA, in addition to it its intelligence mission, has a unique responsibility for developing "standards, techniques, systems, and equipment" for classified information.[40] NSA has demonstrated success at protecting classified systems, but has achieved less success in the increasingly vulnerable area of unclassified computer networks where it plays a supporting role.

Under the 1987 Computer Security Act, the National Institute for Standards and Technology (NIST) was assigned responsibility for developing government wide standards and guidelines for "unclassified, sensitive information."[41] The law also directed NIST to draw upon technical computer security guidelines developed by NSA.[42] To clarify the relationship between NIST and NSA , a Memorandum of Agreement (MOU) was formalized in 1989 establishing mechanisms for implementing the Computer Security Act of 1987. The MOU has been controversial because of concerns in Congress and elsewhere that it cedes NSA much more authority than was intended under the act.[43] The act envisioned NIST requesting NSA expertise as needed, but instead the MOU has involved NSA in all NIST activities related to information security.

Protecting unclassified, sensitive information is essential in developing an effective IW architecture. Given the growing threat to our information system, NSA officials are lobbying for

increased efforts to protect unclassified networks .[44] While NSA certainly has tremendous expertise and is the national authority on cryptographic protection, there are reservations about having it assume a greater role. Some perceive a conflict of interest between NSA's information protection role and its principal intelligence mission. Additionally, leadership in cryptography does not imply leadership in other areas of defensive IW. DOD has assigned the responsibility of protecting its own information infrastructure to the Defense Information Systems Agency.[45] As national defensive IW policy is formulated, the security of unclassified, sensitive information must be addressed.

Non DOD Organizations: Although defensive IW has not been officially embraced outside of DOD, several standing organizations focus on this issue. The National Communication System (NCS) was established in 1963 to coordinate the planning of national security and emergency preparedness communications for the federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. The NCS receives policy direction directly from the National Security Council (NSC) but is managed through the Department of Defense.[46] The NCS's National Coordinating Center for Telecommunications is staffed full time by both government and telecommunications industry representatives whose mission is to respond to both military and civil emergencies: eg., Desert Storm, Hurricane Andrew and, more recently, the bombing of the Federal building in Oklahoma City.[47]

The National Security Telecommunications Advisory Council (NSTAC) was established during the Reagan Administration to advise the President on national security and emergency preparedness issues. This senior body is composed of presidents and CEOs of major telecommunications and defense information systems companies. NSTAC works closely with NCS.

The Federal Communications Commission (FCC) also plays a strong role in reliability and privacy issues regarding the public switched telephone network. The Network Reliability Council (NRC) was created in 1992 by the FCC to investigate the reliability of the public switched network following a series of service outages in 1991. The efforts culminated in a one-thousand page document, "Network

Reliability." The FCC expanded the membership of the NRC in July 1994 and gave it a new charter. Today the NRC is composed of CEOs from telephone companies, equipment suppliers, state agencies, and federal, corporate, and consumer users.

Each of these organizations, as well as NIST, are involved in aspects of defensive IW. What is lacking, however, is an overarching framework linking these disparate efforts into a coordinated effort. Within the government someone needs to be in charge. The NCS may serve as a blueprint for this effort. Not only does it have in place representatives and links to all major government agencies, including the Intelligence Community, but it is a model for government-industry cooperation. To be successful, defensive IW must have the support of private industry. Not only must awareness of vulnerabilities be increased, but coordinated steps taken to reduce the risk. That is the exactly the success which NCS has achieved in the telecommunications sector. As national policy is developed for IW, strong consideration should be given to creating an organization like the NCS to serve as the focal point for this effort and having it possibly work directly for the Vice President. DOD should play a role in the organization but as an active participant, not the leader.

An Azimuth for the Future

There has been a proliferation of IW activities within the Services, OSD, joint activities and defense agencies, but up to this point it has been very decentralized. Revised policy and formal doctrine will go a long way in improving everyone's understanding of IW and their responsibilities. Within the Office of the Secretary of Defense (OSD), one central office needs to remain as the focal point for IW. It is important that the offensive and defensive dimensions of IW are fully coordinated and it made clear to everyone in the department and in the interagency arena who has the lead in OSD. This can be helped through strong leadership by the IW Executive Board.

Similarly on the Joint Staff, a single office needs to be designated as the locus for IW related issues. The central clearing house should be the, J3, Director for Operations. While both the J6 and J2

play key roles in the areas of defensive IW and intelligence support respectively, to be successful, IW must be integrated into operations and that is the purview of the J3. Given the complexity and sensitivity of the issues involved with IW, a flag officer within the J3 should be assigned full time to oversee the development of policy, doctrine, operational planning and the IW component of the Joint Warfighting Capability Assessment. IW has enormous potential for the joint warfighter. A flag officer focusing on this issue will ensure the joint perspective and associated equities are skillfully articulated as this concept is hotly debated within DOD and the interagency process.

At the joint level, strong consideration should be given to more effectively leveraging the capabilities of the Joint Command and Control Warfare Center, Joint COMSEC Monitoring Activity and the Joint Spectrum Center. Each of these organizations is a field operating agency of the Joint Staff and brings a unique dimension to IW. However, aside from informal coordination, no formal mechanism or oversight exists to ensure they provide optimum IW support to the CINCs. For example, while the JC2WC was recently designated responsibility for the joint "Red Team"mission, the Joint COMSEC Monitoring Activity already contains the nucleus for an effective joint "Red Team" capability, with responsibility for monitoring DOD automated information systems and related noncommunications signals. At the same time, close coordination is essential between the Joint Spectrum Center and the JC2WC regarding the Joint Restricted Frequency List and its impact on the planning and conduct of electronic warfare.

The Joint Staff needs to capitalize on the full potential of each of these organizations and ensure there is unity of effort in planning and executing IW. Serious consideration should be given to creating an umbrella Joint Information Warfare Activity with the JC2WC, JCMA, JSC and any other related activities, as subordinate elements. The flag officer position now assigned to the Joint C2W Center should be reallocated to provide senior leadership at the Joint IW Center. Working directly for the Director for Operations on the Joint Staff, he can ensure the Combatant Commands leverage the full potential of IW.

While each of the Services has undertaken a different organizational response to IW, these activities are critical in laying the foundation. They serve as the nucleus upon which the Services can build their respective IW architectures. These organizations will almost certainly evolve over time, but the initial framework is in place. Training the force, particularly operators and system administrators on the defensive aspects of IW, must be tackled in the near term and enable the military to function more effectively in this new environment.

While it may be premature to specify a structure at the interagency level, the National Communication System model cannot be overlooked. Staffed with full time government and telecommunications industry representatives, the NCS serves as a microcosm of the effort that is needed to truly implement a comprehensive national defensive IW campaign. Just as within DOD, there needs to be a focal point to function as the national information assurance coordinator within the government as a whole. Chronic vulnerabilities in the NII must be addressed and coordinated actions undertaken, not only in the telecommunications and automation industries, but across the spectrum of activities involving finance, transportation, power generation and most certainly the military.

Summary

IW clearly offers enormous potential and has become a critical issue for DOD and the U.S. Government. The difficulty that currently exists is the absence of a coherent IW architecture. This paper has focused on the status of the organizational component of that architecture. While significant progress in this area has been achieved within DOD since the concept of IW was formally launched in December 1992, much more work remains to be done. Within DOD the primary focus must be on supporting the joint warfighter and in this regard the existing organizational structure must be streamlined. While offensive IW remains within DOD's realm, defensive IW is truly a national issue and must involve the private sector. The interagency arena is absolutely critical to the success of defensive IW. While DOD can be a major player in this area, it can not lead. Leadership in this area must come from the White House. IW is emerging as an inexpensive, yet effective means to directly

target the U.S. homeland. The U.S. must plan for this contingency in a coherent and coordinated manner and a sound organizational underpinning is a fundamental pillar to both a DOD and national IW architecture.

ENDNOTES

1.Neil Munro, "U.S. Boosts Information Warfare Initiatives," Defense News, 25-31 January 1993, 1.

2.U.S. Department of Defense, Defense Science Board, Report of the Defense Science Board Summer Study Task Force on Information Architecture For the Battlefield, (Washington: Office of the Under Secretary of Defense For Acquisition & Technology, October 1994), B-16.

3."The Defense Science Board (DSB) is a Federal Advisory Committee established to provide independent advise to the Secretary of Defense. Statements, opinions, conclusions and recommendations in the report do not necessarily represent the official position of the Department of Defense." Defense Science Board, inside front cover.

4.Ibid., ES-2.

5.C4 Architecture & Integration Division, the Joint Staff, C4I for the Warrior, (Washington: Joint Staff, 12 June 1992), 1.

6. The NII is "the satellite, terrestrial, and wireless technologies that deliver content to homes, businesses, and other public and private institutions...It is the computers, televisions, telephones, radios, and other products that people employ to access the infrastructure." United States Council on National Information Infrastructure, Common Ground: Fundamental Principles for the National Information Infrastructure, (Washington: U.S. Department of Commerce, March 1995), 1.

7.Science Applications International Corporation (SAIC), Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance, (Vienna, VA: SAIC, 4 July 1995), 1-1.

8.Defense Science Board, B-3-4.

9.Joint Pub 3-13, I-4.

10.Defense Science Board, B-3-4.

11.C2W is defined as, "The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction mutually supported by intelligence to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions." Col Jim Gray, USAF, "Turning Lessons Learned into Policy," Journal of Electronic Defense, no. 10, October 1993, 88.

12.LTGen James R. Clapper and LTC Eben H. Trevino, Jr., "Critical Security Dominates Information Warfare Moves," Signal, March 1995, 71.

13. The most recent draft of C2W doctrine states, "C2W is a warfighting application of IW in military operations and is a subset of IW." Joint Chiefs of Staff, Joint Doctrine For Command and Control Warfare (C2W), Joint Publication 3-13, (Washington: Joint Chiefs of Staff, coordination draft, May 1995), I-2.

14.Ibid., I-6.

15.Ibid., I-4.

16.SAIC, A-11.

17.Robert McNamara, In Retrospect: The Tragedy and Lessons of Vietnam, (New York: Random House, 1995), 108.

18.The Rand Corporation wargame entitled, "The Day After...In Cyberspace" depicted Iranian computer terrorists using Internet to wreck havoc on the U.S. information infrastructure (phone system, power grid, air traffic control) as Iran posed to invade Saudi Arabia. Neil Munro, "Infowar Disputes Stall Defense Policy"; A detailed discussion of the scenario with day by day events is contained in the article by Douglas Waller, 44-46.

19.Defense Science Board, B-11.

20.Neil Munro, "Hacker Attacks Illustrate Vulnerability of DoD War Plans," Washington Technology, 25 August 1994, 18.

21.Armaud de Borchgrave, "Air base no match for boy with modem," Washington Times, 3 November 1994, 1.

22.Ibid., A-12.

23.LTGen James R. Clapper, 72.

24.Bob Woodward, The Commanders, (New York: Simon & Schuster, 1991), 327.

25.Defense Science Board, B-3.

26.Previously designated the Joint Electronic Warfare Center, under the new charter the organization's responsibilities are expanded to incorporate all the dimensions of C2W. Joint Chiefs of Staff, Charter for the Joint Command and Control Warfare Center, CJCSI 5118.01 (Washington: Joint Chiefs of Staff, 15 September 1994), 1.

27.Although the Director, JC2WC is open to a flag officer from each of the Services, habitually the position is filled by an Air Force general officer who is dual hatted as Commander of the Air Intelligence Agency collocated at Kelly Air Force Base, San Antonio, TX.

28.Combatant Commands also receive support from the Joint Communications Security Monitoring Activity and the Joint Spectrum Center. These specialized organizations provide personnel to the CINCs upon request.

29.Vice Admiral J.M.McConnell, Director, NSA, memo "Joint COMSEC Monitoring Activity (JCMA) Concept of Operations (CONOP)," National Security Agency, 19 July 1993, 3.

30.Ibid.

31.General Ronald R. Fogelman, 1.

32."Information Dominance Edges Toward New Conflict Frontier," Signal, August 1994, 37.

33.Steven Watkins, "New Era Had Humble Start," Air Force Times, 20 November 1995, 24.

34.Ibid.

35.Ibid.

36.Robert Holzer, "U.S. Navy Begins Information War Effort, Defense News, 29 August-4 September 1994, 4.

37.Robert Holzer, "Navy Eyes Single Command to Guide Info Warfare," Navy Times, 6 February 1995, 35.

38.SAIC, A-25.

39."Boorda and Mundy Sign Information Warfare Guidance," Inside the Navy, 3 April 1995, 11.

40.Congress, Office of Technology Assessment, Information Security and Privacy in Network Environments,103d Cong., 2d sess., 1994, 143.

41.Ibid., 61.

42.Ibid.,146.

43.The MOU authorizes NIST and NSA to establish a Technical Working Group (TWG) to "review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information." The TWG has six members; three from NIST and three selected by NSA. Ibid.,148.

44.Neil Munro, "Hacker Attacks Illustrate Vulnerability of DoD War Plans," 18.

45.Defense Management Review Decision (DMRD) 918, September 1992, designated the Director, DISA, as the central manager of the DII. SAIC, A-37.

46.Congress, Office of Technology Assessment, Information Security and Privacy in Network Environments, 61.

47.Michael Higgins (higgins@cc.ims.disa.mil), "NII Security: The Federal Force June 5 1995," electronic mail message to Billy Hogan (hoganbilly@aol.com), 6 June 1995.

BIBLOGRAPHY

"Boorda and Mundy Sign Information Warfare Guidance." Inside the Navy, 3 April 1995, 11.

Borchgrave, Arnaud de. "Air base no match for boy with modem." Washington Times, 3 November 1994, 1.

Clapper, James R., LTGen and LTC Eben H. Trevino, Jr. "Critical Security Dominates Information Warfare Moves." Signal, March 1995, 71.

Fogelman, Ronald R., Generall and Sheila E. Widnall. Cornerstones of Information Warfare. Washington: U.S. Department of the Air Force, September 1995.

Gray, Jim, Col. "Turning Lessons Learned into Policy." Journal of Electronic Defense, no. 10, October 1993, 87-92.

Higgins, Michael. (higgins@cc.ims.disa.mil). "NII Security: The Federal Force June 5 1995." electronic mail message to Billy Hogan (hoganbilly@aol.com, 6 June 1995.

Holzer, Robert. "Navy Eyes Single Command to Guide Info Warfare." Navy Times, 6 February 1995, 35

_____. "U.S. Navy Begins Information War Effort." Defense News, 29 August-4 September 1994, 4.

"Information Dominance Edges Toward New Conflict Frontier." Signal, August 1994, 37.

McNamara, Robert. In Retrospect: The Tragedy and Lessons of Vietnam. New York: Random House, 1995.

Munro, Neil. "Hacker Attacks Illustrate Vulnerability of DoD War Plans." Washington Technology, 25 August 1994, 18.

_____. "U.S. Boosts Information Warfare Initiatives." Defense News, January 25-31, 1993, 1.

Joint Chiefs of Staff. Charter for the Joint Command and Control Warfare Center. CJCSI 5118.01. Washington: Joint Chiefs of Staff, 15 September 1994.

_____. Joint Doctrine For Command and Control Warfare (C2W). Joint Publication 3-13. Washington: Joint Chiefs of Staff, coordination draft, May 1995.

Science Applications International Corporation (SAIC). Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Vienna: VA: SAIC, 4 July 1994.

U.S. Congress, Office of Technology Assessment. Information Security and Privacy in Network Environments. 103d Cong., 2d sess. Washington: Government Printing Office 1994.

_____. Information Security and Privacy in Network Environments OTA Report Summary. 103d Cong., 2d sess. Washington: Government Printing Office 1994.

U.S. Council on National Information Infrastructure. Common Ground: Fundamental Principles for the National Information Infrastructure. Washington: U.S. Department of Commerce, March 1995.

U.S. Department of Defense, Commission on Roles and Missions of the Armed Forces. Directions for Defense. Washington: Department of Defense, May 1995.

U.S. Department of Defense, Defense Science Board. Report of the Defense Science Board Summer Study Task Force on Information Architecture For the Battlefield. Washington: Office of the Under Secretary of Defense For Acquisition & Technology, October 1994.

Waller, Douglas. "Onward Cyber Soldiers." Time, 21 August 1995, 38-46.

Watkins, Steven. "New era has humble start." Air Force Times, November 1995.

Woodward, Bob. The Commanders. New York: Simon & Schuster, 1991.